UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,820	10/31/2001	Richard Paul Tarquini	10017334-1	4709

22879 7590 06/14/2010

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2433	

NOTIFICATION DATE	DELIVERY MODE
06/14/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD PAUL TARQUINI and RICHARD LOUIS SCHERTZ

Appeal 2009-006263
Application 10/003,820[1]
Technology Center 2400

Decided: June 10, 2010

Before JOHN A. JEFFERY, JEAN R. HOMERE, and JAMES R. HUGHES, *Administrative Patent Judges*.

HOMERE, *Administrative Patent Judge*.

DECISION ON APPEAL

---

[1] Filed on October 31, 2001. The real party in interest is Hewlett-Packard Development Co., L.P. (Br. 2.)

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) (2002) from the Examiner's non-final rejection of claims 1 through 20. (Br. 3.) We have jurisdiction under 35 U.S.C. § 6(b) (2008).

We affirm-in-part.

Appellants' Invention

Appellants invented a method, apparatus, and computer-readable medium for optimizing performance of signature rule matching in a network. (Spec. 1, ll. 11-13.) According to Appellants, the claimed invention employs a network intrusion prevention system ("IPS") that optimizes a set of machine-readable signatures utilized during frame and packet analysis, thereby reducing the number of signature files checked for unauthorized or malicious activity. (*Id.* at 20, ll. 28-31.)

Illustrative Claims

Independent claims 1 and 13 further illustrate the invention as follows:

> 1. A node of a network for managing an intrusion protection, system, the node comprising:
>
> a memory module for storing data in machine-readable format for retrieval and execution by a central processing trait; and
>
> an operating system comprising a network stack comprising a protocol driver and a media access control driver and operable to execute an intrusion protection system management application, the management application operable to receive text-file input, from an input device, the text file defining a network-exploit rule and comprising at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule.

13. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading input from an input device of the computer;

compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field;

evaluating the machine-readable signature file; and

determining the value of the at least one field of the machine-readable signature file.

Prior Art Relied Upon

The Examiner relies on the following prior art as evidence of unpatentability:

Vaidya	6,279,113 B1	Aug. 21, 2001
Farley	2002/0078381 A1	Jun. 20, 2002

Rejections on Appeal

The Examiner rejects the claims on appeal as follows:

Claims 1 through 7 and 18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Farley and Vaidya.[2]

[2] The Examiner appears to have rejected dependent claim 18 under 35 U.S.C. § 102(e) as being anticipated by Farley. (Ans. 6, 10.) We nonetheless treat dependent claim 18 as being rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Farley and Vaidya in view of its dependence from independent claim 1. (*Id.* at 3.) Appellants failed to object on appeal to the Examiner's omission of dependent claim 18 as being rejected under 35 U.S.C. § 103(a). Therefore, Appellants have waived any

Claims 8 through 17, 19, and 20 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Farley.

Appellants' Contentions

1. Appellants contend that Farley discloses a database that contains information for comparing and detecting events that are indicative of malicious behavior. (Br. 12.) In particular, Appellants argue that Farley's disclosure of evaluating all raw events against all rules defined in the database does not teach "[a] text-file defining a network-exploit …," as recited in independent claim 1. (*Id.* at 12-13.)

2. Appellants contend that Farley's disclosure of a database that includes rules for ranking risk or correlating raw events does not teach a database comprising a value of an ENABLED field or a SEVERITY field. (App. Br. 21.) Further, Appellants argue that Farley's disclosure of raw events that contain parameters relating to the activity within a monitored computer system does not teach machine-readable logic representative of a network-exploit rule. (*Id.*) Thus, Appellants allege that Farley does not teach "compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field," as recited in independent claim 13. (*Id.*)

Examiner's Findings and Conclusions

1. The Examiner finds that Farley's disclosure of classifying and categorizing event information according to an event type, whereby the event information is stored in a database, teaches "defining a network-

---

such arguments on appeal. *In re Watts*, 354 F.3d 1362, 1367 (Fed. Cir. 2004).

exploit rule," as claimed. (Ans. 11.) The Examiner also finds Farley's disclosure of a relationship between event types and correlation rules teaches "defining a network-exploit rule," as claimed. (*Id.* at 11-12.) Further, the Examiner finds that Farley's event information is a data structure that contains fields, including descriptions and values. (*Id.* at 12.) Additionally, the Examiner finds that Farley's disclosure of a security management system that processes correlation events by comparing priority values, original values, and adjusted values teaches "at least one field that includes information from which a determination is made as to whether an intrusion protection system evaluates the network-exploit rule," as claimed. (*Id.*)

2. The Examiner maintains that Farley's disclosure of a relationship between event types and correlation rules teaches "defining a network-exploit rule," as claimed. (*Id.* at 21.) Additionally, the Examiner finds that Farley's disclosure of a vulnerability status consisting of vulnerable, not vulnerable, or unknown teaches "an ENABLED field" value, as claimed. (*Id.* at 21.) Further, the Examiner finds that Farley's disclosure of comparing an historical frequency value against a threshold in order to determine if a raw event is malicious teaches "a SEVERITY field" value, as claimed. (*Id.* at 21-22.) The Examiner also finds that Farley's disclosure of assigning status values ranging from 1 to 3 also teaches "a SEVERITY field" value, as claimed. (*Id.* at 22.)

II. ISSUES

1. Have Appellants shown that the Examiner erred in concluding that the combination of Farley and Vaidya renders independent claim 1 unpatentable? In particular, the issue turns on whether the proffered

combination teaches a management application operable to receive from an input device text-file input defining a network-exploit rule, as recited in independent claim 1.

2, Have Appellants shown that the Examiner erred in finding that Farley anticipates independent claim 13? In particular, the issue turns on whether Farley teaches "compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field," as recited in independent claim 13.

III. FINDINGS OF FACT

The following Findings of Fact ("FF") are shown by a preponderance of the evidence.

Farley

1. Farley discloses "a computer security management system that can log, investigate, respond, and track computer security incidents that can occur in a network computer system." (3: para. [0045].) In particular, Farley discloses a fusion engine that classifies real-time computer events and, further, ranks the real-time computer events based upon a comparison with one or more databases. (*Id.*)

2. Farley's Figure 6 depicts components of the fusion engine (22). (7: para. [0085].) In particular, Farley discloses that the fusion engine (22) includes an event reader (600). (8: para. [0093].) Farley discloses that "[t]he event reader *600* can receive raw computer events from either the event collector *24* or an event log file *610*." (*Id.*) Further, Farley discloses

the event log file (610) comprises multiple files, whereby the files consist of comma separated values ("CSV") formats that store computer event data. (*Id.*) Additionally, Farley discloses that the event reader (600) creates raw event data objects that are capable of being processed by other software components within the fusion engine (22). (*Id.*)

3. Farley's Figure 6 depicts that the fusion engine (22) also contains one or more correlation rules (620) that utilize algorithms to determine the occurrence of a security incident (8: para. [0089].) Farley discloses that the fusion engine (22) contains a controller (655) that loads a correlation rule (620) during system initialization. (16: para. [0184]. In particular, after receiving a raw event, the event reader (600) determines the applicable correlation rules (620) by retrieving both the raw event's event type and the event type's list of pertinent rules. (*Id.*)

4. Farley's Figure 5B depicts an exemplary raw event (505) which comprises a priority status parameter (535) assigned by a detector within the intrusion detection system. (6-7: para. [0076]; 14: para. [0161].) Farley discloses that the priority status parameter comprises one of the following three values: 1, 2, or 3. (14: para. [0161].) Farley discloses that the highest priority value is 1, while the lowest priority value is 3. (*Id.*)

5. Farley's Figure 11 depicts a computer-implemented process that adjusts the priority status of a raw event based upon the CoBRA-assigned context parameters. (13: para. [0159].) In step 1155, the computer-implement process determines whether the frequency of the current raw event being evaluated exceeds a frequent event threshold and, therefore, amounts to a non-malicious event. (15: para. [0171].)

IV. ANALYSIS

35 U.S.C. § 103(a) Rejection

Claim 1

Independent claim 1 recites, in relevant part, a management application operable to receive from an input device text-file input defining a network-exploit rule.

As detailed in the Findings of Fact section, Farley discloses a computer security management system that includes a fusion engine capable of classifying and ranking security incidents. (FF 1.) In particular, Farley discloses that the fusion engine includes an event reader that receives computer events from an event log file. (FF 2.) Farley discloses that the event log file comprises multiple files formatted to store computer event data. (*Id.*) Further, Farley discloses that the fusion engine contains one or more correlation rules for evaluating security incidents. (FF 3.) Farley discloses that the fusion engine includes a controller for loading the correlation rules during system initialization. (*Id.*) Once the correlation rules are loaded, the event reader determines which correlation rules pertain to each computer event based on the event type. (*Id.*)

We find that Farley's disclosure teaches a computer security system that includes a fusion engine which utilizes correlation rules to evaluate multiple text files formatted to store computer event data. In particular, we find that Farley's fusion engine receives text files that store computer event data and separately loads correlation rules during system initialization. However, we find that Farley's cited disclosure falls short of teaching or suggesting an IPS operable to receive from an input device a *text file* defining a network-exploit rule, as claimed. Although we find that Farley's

disclosure teaches that the fusion engine loads correlation rules during system initialization, Farley's cited disclosure does not teach that the fusion engine, when operating, is capable of receiving a text file from an external device that defines a correlation rule. While Farley's fusion engine may be able to define a correlation rule, we find that such correlation rule is not a text file received from an input device. Therefore, the Examiner has improperly relied upon Farley's disclosure to teach the disputed limitation. Further, we find that Vaidya does not cure the noted deficiencies of Farley.

Since Appellants have shown at least one error in the Examiner's rejection of independent claim 1, we need not reach the merits of Appellants' other arguments. It follows that Appellants have shown that the Examiner erred in concluding that the combination of Farley and Vaidya renders independent claim 1 unpatentable.

Claims 2 through 7 and 18

Because dependent claims 2 through 7 and 18 also recite the limitation discussed above, we find that Appellants have also shown error in the Examiner's rejection of these claims for the reasons set forth in our discussion of independent claim 1.

35 U.S.C. § 102(e) Rejection

Claims 8 through 12, 19, and 20

Because independent claim 8, and dependent claims 9 through 12, 19, and 20, also recite the limitation discussed above, we find that Appellants have also shown error in the Examiner's rejection of these claims for the reasons set forth in our discussion of independent claim 1.

Claim 13

Independent claim 13 recites, in relevant part, "compiling the input into a machine-readable signature file comprising machine-readable logic representative of a network-exploit rule and a value of at least one field selected from the group consisting of an ENABLED field and a SEVERITY field."

As detailed in the Findings of Fact section above, Farley discloses assigning a priority status parameter to each computer event. (FF 4.) In particular, Farley discloses that the priority status parameter ranges from 1 to 3, whereby 1 indicates the highest priority. (*Id.*) Further, Farley discloses that the fusion engine includes a CoBRA processor which adjusts the priority status of a computer event by determining if the computer event exceeds a frequency threshold. (FF 5.) Farley discloses that computer events which exceed the frequency threshold amount to non-malicious events. (*Id.*)

We find that Farley's disclosure teaches that the fusion engine assigns a priority value to each text file that stores a computer event, and compares the priority value to a predetermined frequency threshold. As set forth above, we find that Farley's disclosure teaches that the fusion engine loads correlation rules during system initialization. In particular, we find that Farley's disclosure of the fusion engine loading correlation rules, in conjunction with assigning a priority value to each text file, amounts to compiling software functions pertaining to a correlation rule and a priority value. Thus, we find that Farley's disclosure teaches the disputed limitation. It follows that Appellants have not shown that the Examiner erred in finding that Farley anticipates independent claim 13.

Claims 14 and 16

Appellants do not provide separate arguments for patentability with respect to dependent claims 14 and 16. Therefore, we select independent claim 13 as representative of the cited claims. Consequently, Appellants have not shown that the Examiner erred in rejecting dependent claims 14 and 16 for the reasons set forth in our discussion of independent claim 13. *See* 37 C.F.R. § 41.37(c)(1)(vii) (2009).

Claims 15 and 17

Appellants do not set forth any substantive arguments, but rather make a general allegation that Farley's cited disclosure does not teach the language of dependent claims 15 and 17. (Br. 22-23.) Appellants are reminded that a statement that merely points out what the claim recites will not be considered as an argument for separate patentability of a claim. 37 C.F.R. § 41.37(c)(1)(vii). Therefore, Appellants' arguments are unpersuasive. It follows that Appellants have not shown that the Examiner erred in finding that Farley anticipates dependent claims 15 and 17.

VI. CONCLUSIONS OF LAW

1. Appellants have shown that the Examiner erred in rejecting claims 1 through 7 and 18 as being unpatentable under 35 U.S.C. § 103(a).

2. Appellants have shown that the Examiner erred in rejecting claims 8 through 12, 19, and 20 as being anticipated under 35 U.S.C. § 102(e).

3. Appellants have not shown that the Examiner erred in rejecting claims 13 through 17 as being anticipated under 35 U.S.C. § 102(e).

VII. DECISION

1. We reverse the Examiner's decision to reject claims 1 through 7 and 18 as being unpatentable under 35 U.S.C. § 103(a).

2. We reverse the Examiner's decision to reject claims 8 through 12, 19, and 20 as being anticipated under 35 U.S.C. § 102(e).

3. We affirm the Examiner's decision to reject claims 13 through 17 as being anticipated under 35 U.S.C. § 102(e).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a).

AFFIRMED-IN-PART

Vsh

HEWLETT-PACKARD COMPANY
INTELLECTUAL PROPERTY ADMINISTRATION
3404 E. HARMONY ROAD
MAIL STOP 35
FORT COLLINS, CO 80528